Introduction – Malicious Website Verification

Following this procedure will determine if a website is actually malicious or being used for malicious purpose(s). Based on this analysis, determine if an incident has possibly occurred and begin the next appropriate procedure.

Instructions

A. Use these selected URL reputation tools below, to investigate what our security partners, other vendors, and other companies have discovered about the site. These URL reputation tools will identify:

- The category of the URL and if it has deemed malicious.
- Detection and analysis of web-based malware.
- Analyze files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners

***If an URL is a shortening service provider e.g. tinyURL, goo.gl url, bitly, owly, or other TLD service provider:

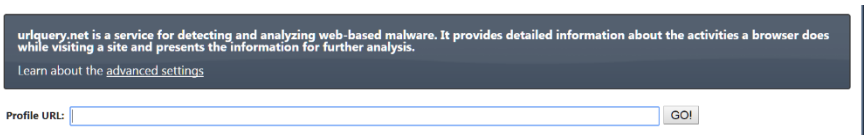
- Expand shortened url first, and proceed with the rest of the work instruction. (Example of url expander service site; http://urlex.org/)

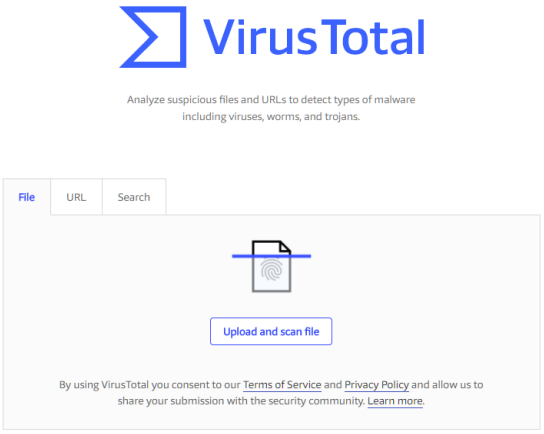
- https://fortiguard.com/webfilter
  *The category of the URL and if it's deemed malicious

- https://virustotal.com or https://urlquery.net or https://urlscan.io

*Detection and analysis of web-based malware

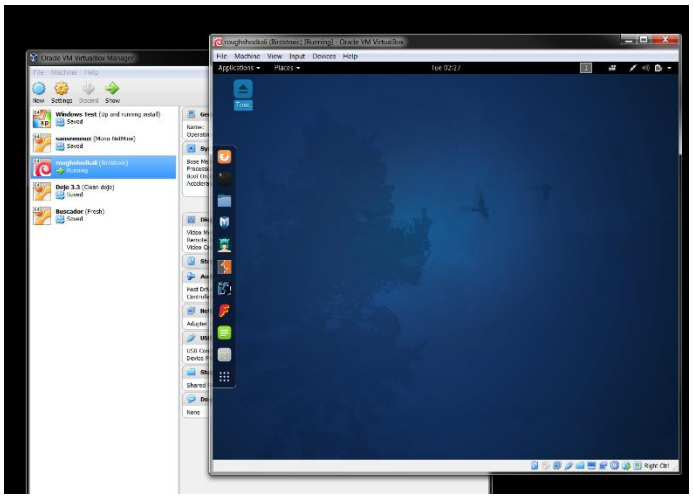
*Analyze files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners



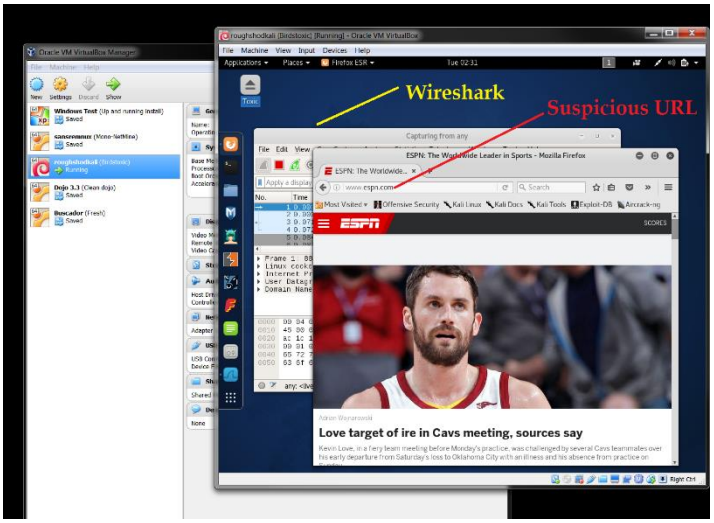


B. Utilize a virtual machine, a dirty laptop connected to the outside internet line, or AWS ec2 instance to visit the URL in question and analyze the URL.

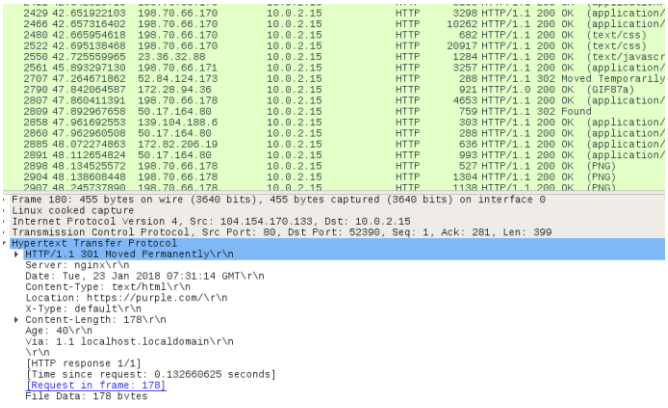
- Load a clean snapshot of Window or Linux to a virtual machine



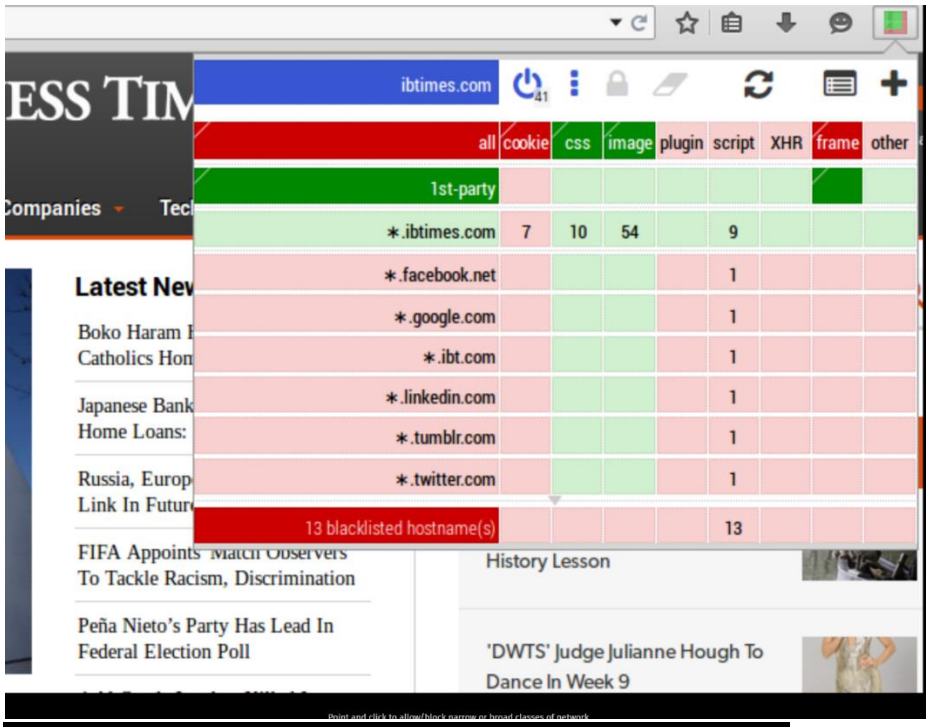
- Start a network packet capture e.g. tcpdump / wireshark
- Visit the URL in question

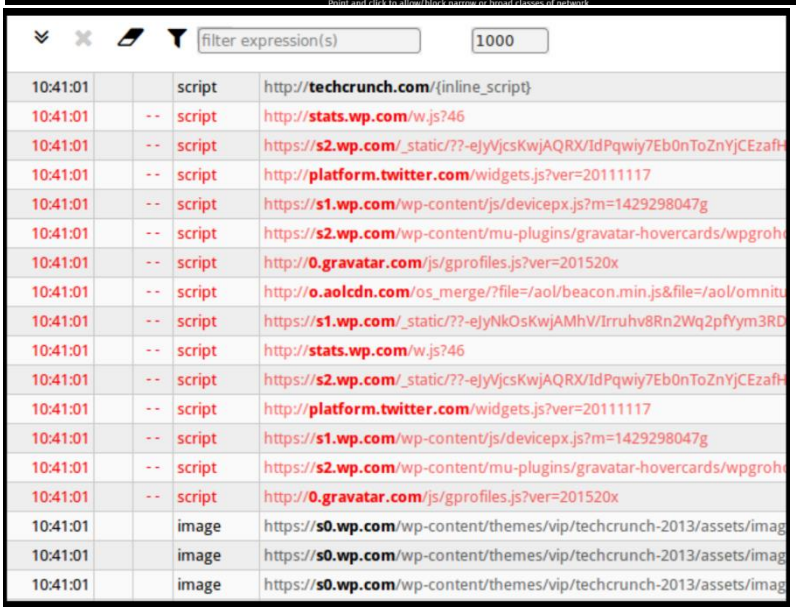


- After 1 minute stop packet capture and examine the packet capture data and/or save packet capture files to be uploaded to static analysis site



C. Use a browser add-on such as uMatrix to see ALL the remote connections, failed or attempted, depending on whether they were blocked or allowed (https://addons.mozilla.org/en-US/firefox/addon/umatrix/)





Checklist – Malicious URL Verification

- Is domain categorized as a known: Phishing, Malicious Websites, Newly Observed Domain, Newly Registered Domain, Spam URLs, Dynamic DNS – hosted site.
- Was suspicious website traffic associated with a known good domain.
- Was suspicious website traffic seen.
- Was suspicious traffic isolated.
- Was there any malware downloaded.
- Was there any redirects or callouts to foreign host(s)

Based on the analysis determine if an incident has possibly occurred and begin the appreciate procedure.